RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: HUM-R05

Taking the Fight Upstream: Pursuing Systemic Defense Against Phishing

MODERATOR:

Tal Goldstein
Head of Strategy
World Economic Forum
Centre for Cybersecurity

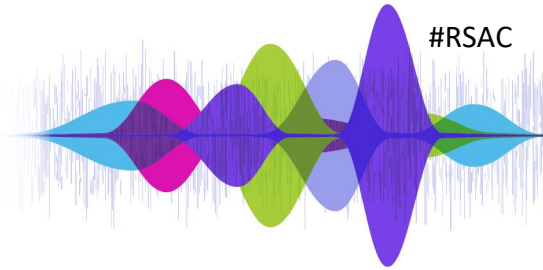
PANELISTS:

Kelly Bissell
CVP Security & Fraud
Microsoft

Steven Kelly
Chief Trust Officer
Institute for Security and Technology

Kemba Walden
President
Paladin Global Institute
Paladin Capital Group

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

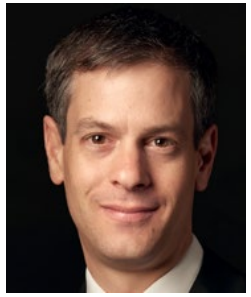
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:



Tal Goldstein

Head of Strategy
World Economic Forum
Centre for Cybersecurity

PANELISTS:

Kelly Bissell

CVP Security & Fraud
Microsoft

Kemba Walden

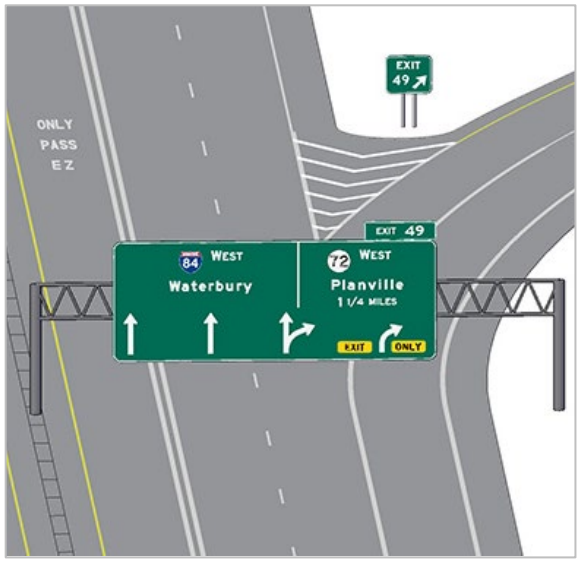
President
Paladin Global Institute
Paladin Capital Group

Steve Kelly

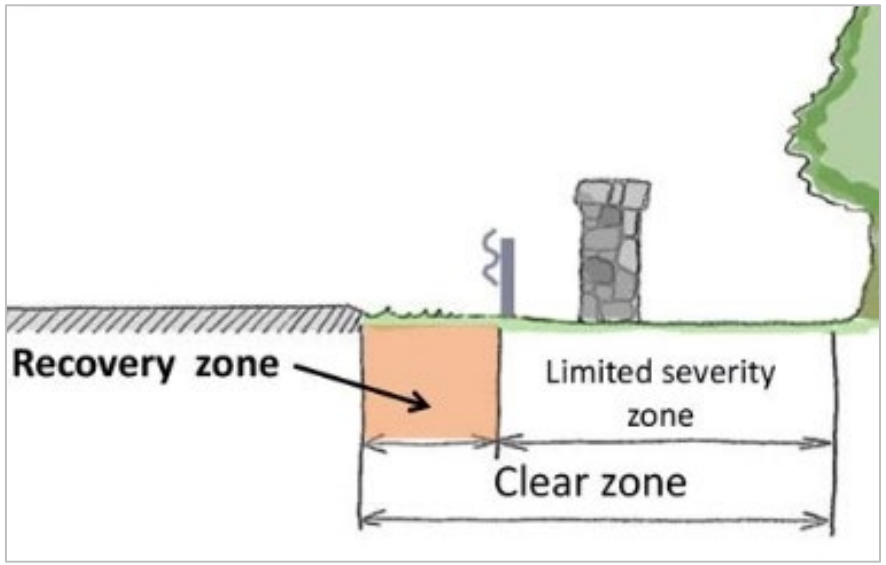
Chief Trust Officer
Institute for Security and Technology

A short story about roadway design…

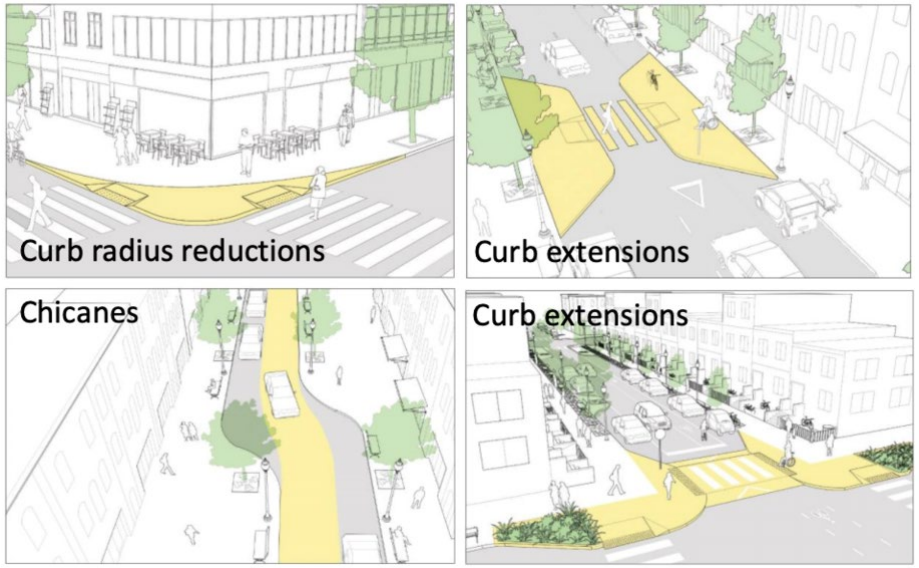
Goal: Minimize the consequences of human errors and crashes by creating road environments that reduce the likelihood of severe injuries or fatalities.



Intuitive Design
(Avoid surprise)

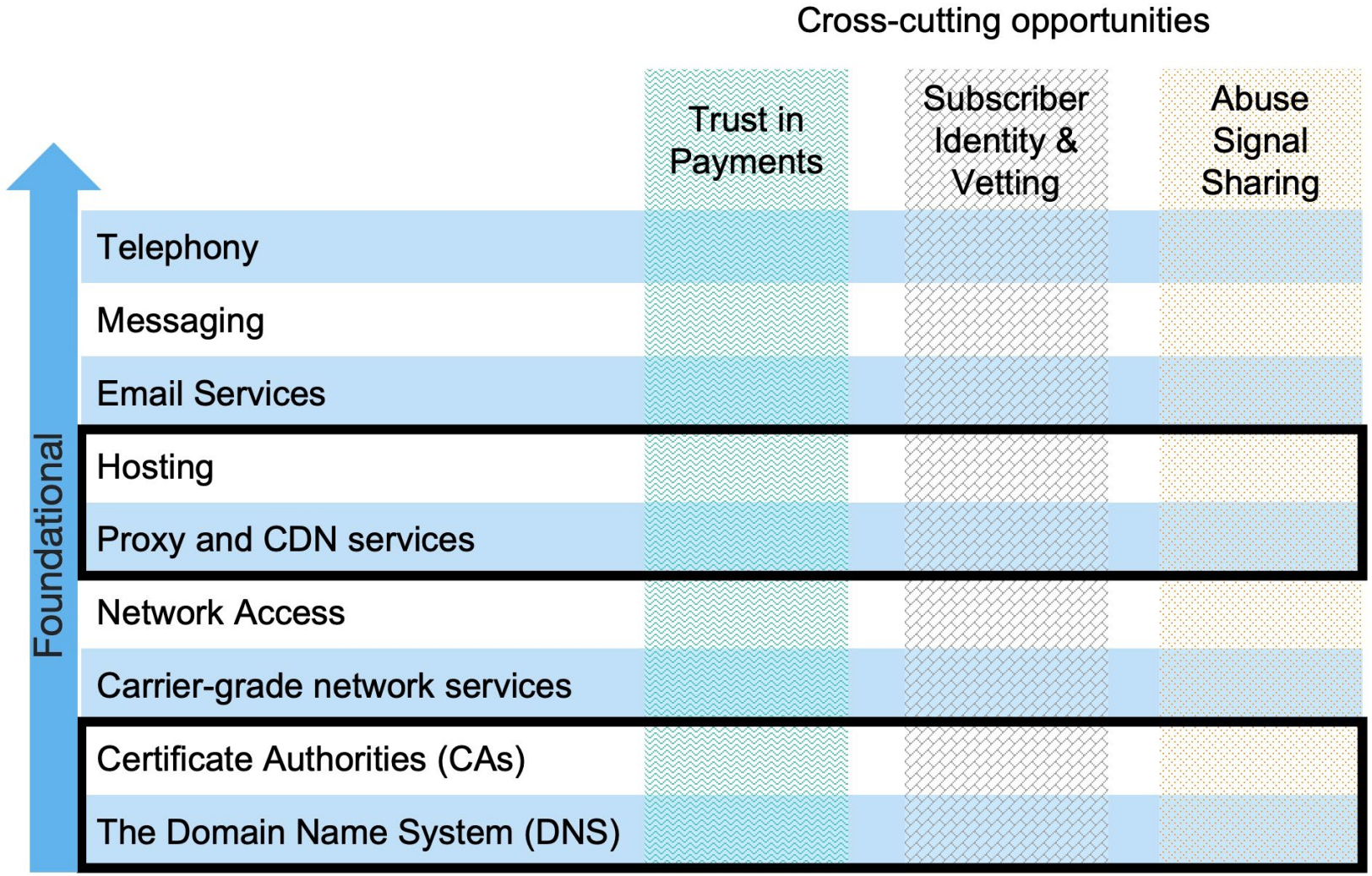


Forgiving Highway Roadsides
(Mitigate consequences of error)



Pedestrian-Oriented Development
(Reduce auto speeds, improve safety)

Can we implement similar design principles in the tech ecosystem?



A “systemic defense” framework

Structurally reduce bad actors’ ability to procure and operationalize cyber infrastructure

Increase trust in the Domain Name System (DNS) by preventing the registration of fraudulent domain names at speed and scale.

Scale adoption of proven counter-measures, such as phishing-resistant MFA, Protective DNS, and DMARC.

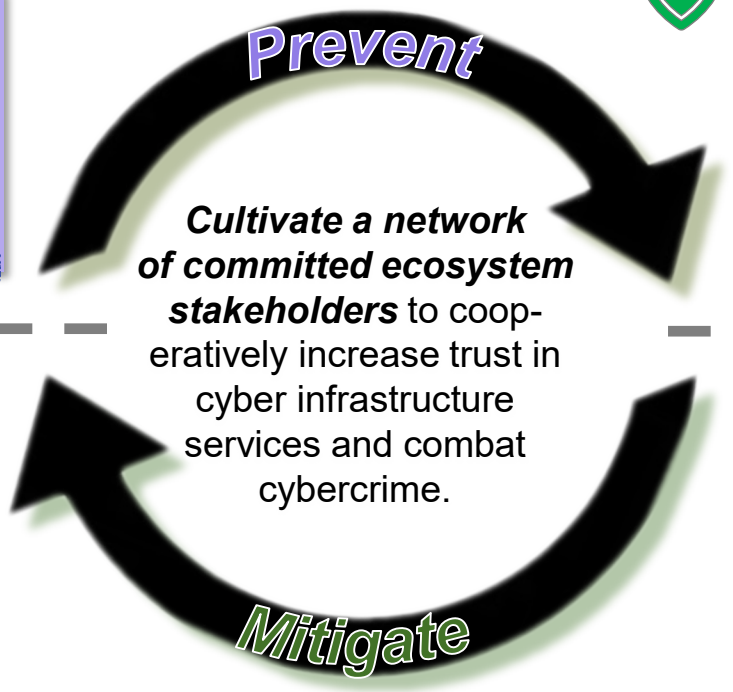
Fully leverage identity as a trust or risk signal in cyber infrastructure transactions, including by harnessing national digital ID initiatives.

Enable and incentivize ecosystem-wide abuse reporting, response, and mitigation efforts

Scale cooperative mechanisms like signal sharing to enable ecosystem-wide awareness, protective measures, and disruptive actions.

Promote cooperative approaches like “trusted reporter” programs to enable abuse reporting and mitigation at speed and scale.

Incentivize responsible business practices, including through a provider-focused reputation ranking system as an additional trust/risk signal.


Prevent
Cultivate a network of committed ecosystem stakeholders to cooperatively increase trust in cyber infrastructure services and combat cybercrime.
Mitigate

Apply What You Have Learned Today

- Next week you should:
  - Reach out if you have suggestions for their approach.
- In the first three months following this presentation you should:
  - Identify ways in which you can incorporate “systemic defense” approaches into your product or service, so it is safe and secure by design.
- Within six months you should:
  - Share your expertise by volunteering within your community or contributing to multi-stakeholder efforts in a standards body, public-private consortium, or research institution.

RSAC™ 2025 Conference

Many Voices.
One Community.

If you have comments or suggestions for the solutions framework, please contact the presenters or:

info@securityandtechnology.org